**Page 1; Problem Domain**

**Page 2; Threat Model**

**Page 3; Hypothesis, Sample Metric**

**Problem Domain:**

*Education.* Specifically, servers containing student and faculty data within a new and (possibly?) improved computer system installed throughout schools under the jurisdiction of the city’s board of education. I want to prove that this partial/limited lack of access to servers lead to compromised data security rather than additional security as intended, which factors into the A of CIA—availability.

The situation is this: The school system restricted access to the school-wide servers to a limited number of teachers in order to boost the secureness of the student’s personal data, likely at the request of parents. However, I think that such an action encourages less secure methods of data-sharing—printing off information and giving it to others, using personal e-mails to send information, etc. Therefore, the system designed to increase security is undermining the security instead through human factors.

**References:**

*(regarding educational data)*

1. H. Alamleh, "Private and Secure Students' Data Sharing in Educational Systems," *2020 Sixth International Conference on e-Learning (econf)*, 2020, pp. 158-161, doi: 10.1109/econf51404.2020.9385450.
2. B. Schneier, "University Networks and Data Security," in *IEEE Security & Privacy*, vol. 4, no. 5, pp. 88-88, Sept.-Oct. 2006, doi: 10.1109/MSP.2006.138.
3. S. Karabatak and M. Karabatak, "Information Security Awareness of School Administrators," *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757525.

*(regarding human factors)*

1. J. Rasmussen, "Human factors in the high-risk systems," *Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants*, 1988, pp. 43-48, doi: 10.1109/HFPP.1988.27474.
2. H. Sarkis, "Getting the attention of senior management for human factors issues: quantitative survey data," *Conference Record for 1992 Fifth Conference on Human Factors and Power Plants*, 1992, pp. 482-487, doi: 10.1109/HFPP.1992.283358.
3. K. Potosnak, "Human factors-management: the key to success," in *IEEE Software*, vol. 6, no. 2, pp. 86-, March 1989, doi: 10.1109/52.23136.

**Threat Model – Persona non Grata (PnG) Model**

**Overview:** This threat model will take place under a system as described in the problem domain—an unsecure system in whichsensitive data is openly shared, and therefore no sophisticated methods are necessarily needed.

**Attacker**: John Smith

**Bio**: John Smith worked at X Public High School as a mathematics department faculty member for 22 years until his recent firing. As a member of the mathematics department, Mr. Smith also oversaw classes in computer skills, and therefore has a working knowledge of computer systems. Mr. Smith was not well-liked by the students and faculty but was confident in his teaching abilities and steadfast in his instruction methods. Despite having tenure, Mr. Smith was fired after an account of an alleged incident reached the ears of the school’s principal. Angry, embarrassed, and feeling vilified in the wider community, Mr. Smith desires revenge on the school system and coworkers who shunned him.

X Public High School has recently adopted a new computer system intended to boost security, however access to the server is limited, and therefore, many teachers share confidential information like student data with one another through e-mail or printed media. Also, as most of the teachers in the school are unfamiliar with the new-and-improved system, they have resorted to methods like writing down passwords, or using their personal e-mail accounts.

**Skills**:

* Advanced mathematics
* Intermediate computer skills

**Goals:**

* To destroy the school’s reputation by releasing sensitive information and exposing the school’s lack of data protection ability to parents and wider community
* To discover and reveal any confidential data that could lead to controversy or PR issues for the school
* To cause confusion and disorder within the school system, and incite an incident that may result in the firing of any number of school officials

**Misuse Cases**:

* Enter faculty computers through written-down passwords and easily enter the server from those computers
* Find or save printed data from himself or other faculty members containing sensitive information
* Using the faculty computers, access personal e-mails and gather sensitive data about the school, students, and faculty
* Check downloads, trash/recycling, and personal folders on each desktop whose password he can find for sensitive data

**Hypothesis**

***If the computer system in the school is secured in a way which prevents users from being able to sufficiently utilize their devices, then human factor/human element will result in decreased security for the entire system.***

My hypothesis is that, by extending server access at the school to all faculty members and amending the system to be more accessible, the data in those servers would be kept more secure. This solution should be common sense, but I think it can be considered different because generally, we think that piling on security measures will make something more secure. And in some cases, that can be true. However, we often forget about the human behind the computer screen; they are often the weakest link in what otherwise may be a perfect security system.

In my specific case, the school thought that the data would be more secure by limiting access and cranking up the security measures like assigning everyone difficult login passwords. But as I mentioned before, I think that this leads to unsecure data sharing instead. Also, tighter security may, at face value, be helpful to keep data safe, but it collapses in on itself when it ill-suits the people who are using it (most people who work at my school are over 50, and the majority can barely use e-mail properly…). In conclusion, I think that data security can only work to its fullest when it takes its human users into account. Availability and useability are often forgotten but are absolutely paramount to data security.

**Sample Metric**

I will use the Cyber Human Error Assessment Tool (CHEAT), which was recently developed as an alternative to current human reliability assessment (HRA) tools such as the Human Error Assessment and Reduction Technique (HEART) that quantifies human factors in cybersecurity assessments. This method asses the risk of human error by collecting data through staff interviews and identifying indicators of risk. These data are then compiled and analyzed to produce a risk assessment and mitigation recommendations. The CHEAT system factors in people, organization, history, technology, and environment. The CHEAT system is good because it focuses on cybersecurity but also because it takes into account the specific circumstances of each company and system.

I can run the risk assessment under the conditions of the old and new security system in order to determine if the risk is higher in the system with limited accessibility.

-----

*Information about CHEAT*

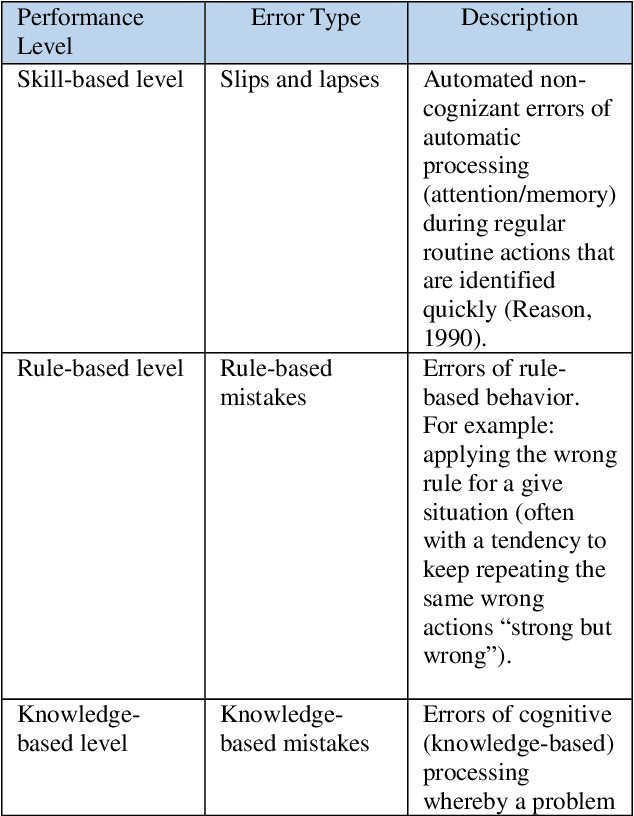
A. J. Widdowson and P. B. Goodliff, "CHEAT, an approach to incorporating human factors in cyber security assessments," 10th IET System Safety and Cyber-Security Conference 2015, 2015, pp. 1-5, doi: 10.1049/cp.2015.0298.https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7792023&isnumber=7332861

-----

*Basic Data Sample*

|  |  |  |
| --- | --- | --- |
| Risk Indicators (from interviews) | Risk Assessment | Risk Score |
| Employees cannot remember passwords, often write them down | High Risk | 3 |
| Employees share sensitive data through personal e-mail | High Risk | 3 |
| Access to employee offices is unrestricted | Moderate Risk | 2 |

*Sample Metric (Historical Technique – HEART Method)*



Alexander, Tiffaney Miller. "Human Error Assessment and Reduction Technique (HEART) and Human Factor Analysis and Classification System (HFACS)." (2017).